

=====

H I P A A L E R T Volume 2 No. 7 May 7, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

=====

HIPAAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total 11,500+!

Do you have interested associates? They can subscribe free at:
<http://www.hipaadvisory.com/alert/>

IF YOU LIKE HIPAAALERT, YOU'LL LOVE HIPAADVISORY.COM! --
Phoenix' comprehensive "HIPAA hub of the Internet," per Modern Healthcare magazine. Visit: <http://www.hipaadvisory.com>

=====

THIS ISSUE

1. From the Editors
 2. HIPAAAlert's Spring HIPAA Progress Survey Results Are In!
 3. HIPAAnews: Privacy Rule -- In Effect, But Still Controversial
 4. HIPAAAdvisor: Of Affiliates and Associates
 5. HIPAAview: Vendors and HIPAA Compliance -- Reality Knocks
- =====

1 / FROM THE EDITORS:

In our healthcare world, the atmosphere is fiery enough to be mistaken for a summer heat wave, despite the early May date. Certainly, the surprising mid-April endorsement by DHHS Secretary Thompson of the Privacy Rule -- even if a qualified endorsement -- seems to have re-charged rather than quelled association-level resistance, enterprise-level controversy, and staff-level confusion.

Has the Administration's decision to go forward on the Privacy Rule also fired industry action? Or, are we -- or some of us -- digging in our heels? Phoenix Health Systems announced its 5th quarterly HIPAA progress survey only days after the decision specifically to find out -- and the results of this largest-ever nation-wide healthcare industry study follow.

Also below...as always, the latest HIPAA headlines...and, in HIPAAAdvisor, Pepper Hamilton attorneys Steve Fox and Rachel Wilson

sort out the differences between "affiliates" and "business associates". Finally in HIPAAviews, Roy Rada, MD, PhD and author of HIPAA@IT, examines vendor "HIPAA compliance" from his eye-opening and eminently practical perspective.

Diane Boettcher, Editor
dboettcher@phoenixhealth.com

D'Arcy Guerin Gue, Publisher
daggue@phoenixhealth.com

=====

2 / NEW NATION-WIDE HIPAA INDUSTRY SURVEY RESULTS

** HIPAA Compliance Efforts: Slow and Spotty, but Strengthening **

It's happening. Slowly, perhaps reluctantly, the healthcare industry just might be making way for HIPAA. An increasing number of healthcare organizations apparently have begun to focus in earnest on HIPAA compliance, according to Phoenix Health Systems' latest quarterly results from the largest-ever nation-wide healthcare industry survey.

Approximately 3/4 of the 600+ survey participants reported that their organizations are actively engaged in enterprise HIPAA awareness efforts, 2/3 are addressing internal impact assessments, about half are working on HIPAA project planning, and roughly a third are making inroads on actual HIPAA implementation.

THE SURVEY

During the last two weeks of April 2001, Phoenix Health Systems conducted its fifth quarterly industry HIPAA compliance survey through its website HIPAAAdvisory.com and HIPAAAlert email newsletter. The 617 online respondents represented:

- > 113 hospitals with 400+ beds
- > 144 hospitals with 400 - beds
- > 28 physician practices
- > 74 other providers
- > 82 payers
- > 10 clearinghouses
- > 58 vendors
- > 108 other (consultants, gov't, assoc)

The majority of respondents, 77%, held official roles in HIPAA compliance within their organizations; about 50% were executives or department managers and another 25% were Compliance or Security

officers for their organizations.

HIPAAWARENESS and the EFFECT OF THE PRIVACY RULE

Across the industry, overall awareness of HIPAA was reported consistently: about 70% of all senior managers were judged as having moderate to high knowledge of HIPAA and its implications. Fewer department heads -- just under 50% -- were reported to have moderate to high awareness. Respondents stated that 6 % of all senior managers across the industry still have little or no knowledge of HIPAA.

When asked if the recent DHHS decision to put the Privacy Rule into effect affected urgency about HIPAA, 41% of hospital respondents and 36% of all respondents answered that their organizations' sense of urgency had increased "quite a lot" or "greatly." Only 6% of respondents believed that their organizations were unaffected by the news of the Privacy rule's effective date, and 14% indicated that their organizations' sense of urgency about HIPAA was already high before the news.

FOCUS OF HIPAA EFFORTS

As summarized earlier, the number of organizations focusing on the components of HIPAA compliance appears to have significantly increased since January. Among hospitals with over 400 beds, about 80% reported they were focusing on impact assessments, primarily in the areas of Transactions and Privacy, and 70% stated they were doing project planning.

Roughly 70% of respondents from hospitals with less than 400 beds reported they were working on impact assessments, with 56% asserting that they were engaged in project planning. However, actual implementation efforts are still to come for most hospitals; fewer than 30% of respondents from larger hospitals, and less than 25% from the smaller hospitals had begun implementation of any HIPAA provisions.

Approximately 30% of all providers expected to complete internal assessments in the next 3 months, and another 43% will complete assessments within 6 months. In our January 2001 survey, we found that only 5% of hospital providers had completed assessments; as of mid-April, this had increased to 11%.

Payers and vendors continued to be ahead of providers in meeting compliance goals. About 75% of payers and 52% of vendors reported working on Transactions-related project planning; and 58% of payers and 62% of vendors stated they were engaged in Transactions implementation activities. About 58% of payers and 46% of vendors reported doing project planning work in Privacy; about 30% of payers and 55% of vendors stated they were implementing the Privacy provisions.

USE OF OUTSIDE EXPERTISE

Among hospitals with over 400 beds, 53% of respondents indicated they would engage outside consultants to support their HIPAA compliance endeavors; 47% of respondents from smaller hospitals reported similar plans. Most likely uses of consultants by hospitals were reported to be: first, compliance planning; second, risk assessment; and third, education management.

Payers are likely to be even stronger users of consultants; 72% of payer respondents reported the engagement of consultants, primarily for help in compliance planning and risk assessments

PROVIDER BUDGETS

Only provider respondents were asked how much their organizations are budgeting for HIPAA compliance in 2001, and their responses varied considerably. Of the 113 participants from hospitals with over 400 beds, 21% did not know budget numbers. Among those knowing their budgets, 22% reported 2001 budgets of less than \$100,000, 53% claimed budgets of between \$100,000 and \$500,000, 18% expect spending between \$500,000 and \$1 million, and 7% stated they would spend over \$1 million.

About 42% of respondents from hospitals with fewer than 400 beds did not know their organizations' 2001 budgets. Among those knowing their budgets, About 2/3 reported that their organizations' budgets were less than \$100,000; 23% cited budgets between \$100,000 and \$500,000, 5% anticipated budgets between \$500,000 and \$1 million, and another 6% said their organizations planned to spend over \$1 million.

Among participants from other provider groups and physician practices, approximately 50% stated they didn't have budget numbers to cite, and most of the remaining respondents indicated they would spend under \$100,000 in 2001 on HIPAA.

READINESS TO DO HIPAA-COMPLIANT BUSINESS

Of the 82 payer organization respondents, 24% indicated they would be ready to accept and transmit their first HIPAA compliant transactions within 6 months, 30% in 6 to 12 months, and 35% in 12 to 18 months. Just under 30% indicated that their organizations would be ready to transmit all HIPAA compliant transactions within a year or less, but 54% won't be ready for 12-18 months, and 18% said they wouldn't achieve this full capability until after the compliance deadline of October 2002.

Vendors reported more confidence in their progress towards HIPAA-related remediation of products. Over 60% reported that they have begun coordinating with their clients on HIPAA, and about 80% said they have made significant progress in complying with HIPAA

requirements. About 30% either had already completed remediation or expected to do so within 6 months; 40% planned to be ready within 6 to 12 months, and about 15% expected it to take longer. Over 80% of vendors stated that they plan to offer HIPAA compliance assistance to their customers.

About 75% of participants from clearinghouses reported that their firms had begun coordinating on HIPAA remediation with their clients. About 40% expected that their compliance activities will require some new software development, and 50% anticipated making changes to their existing software. All clearinghouse respondents indicated that their firms would be ready to transmit all HIPAA compliant transactions within 12 to 18 months, before the Transactions compliance deadline.

PARTICIPANT COMMENTS MAY SAY IT ALL...

Each of Phoenix' quarterly HIPAA surveys invariably generates an array of commentary. The Spring 2001 Survey has been no exception. Some of the more representative comments:

From Hospital respondents:

"Change comes slowly to healthcare."

"...Our top payers aren't ready to work with us on implementation."

"HIPAA will be a long process but well worth the time forming complete confidentiality."

"It is difficult to be the only one in an organization that takes this seriously."

"We need more time!"

From Other Provider respondents:

"Senior management is not planning to address this issue until Summer or Fall 2001 in case things still change."

"I think the whole long-term care industry is behind the curve on HIPAA."

From Vendor respondents:

"How could any vendor be much more than 25% ready when the privacy regulation just went into enactment, security is not final, and none of the identifiers specs are out?"

"We are moving towards education of our staff so there is no

confusion about what we do, and what the customer is required to do. We are not the entity that needs to be HIPAA compliant, the customer(s) must be HIPAA compliant."

From Clearinghouse respondents:

"For transactions/code sets, the impact and effort required is far greater than initial estimates."

"Our biggest holdup is receiving specifications from payers...."

From Payer respondents:

"Healthcare executives relied too much on a pro-business White House...(There is) a lot of denial in this industry..."

"Developing an awareness with our clients and our trading partners is an ongoing, but slow process."

"HIPAA is changing everything in our company...this is a tremendous job to get done in a short time."

For these survey results, including illustrative graphs, visit:
<http://www.hipaadvisory.com/action/survey/spring01.htm>

To review results of our prior quarterly HIPAA surveys, visit:
<http://www.hipaadvisory.com/action/survey/>

=====

3 / H I P A A n e w s

*** Rep. Arney Wants Privacy Reg "Fixed" ***

In a May 2nd letter to DHHS Secretary Thompson, House Majority Leader Dick Arney asked that the HIPAA Privacy Regulations be fixed. The letter quotes a section designed to allow DHHS to "ascertain compliance". Rep. Arney states that this provision gives the government unprecedented access to sensitive medical records.

Arney urged Secretary Thompson to take advantage of his authority to modify the regulations for up to two years after they have been finalized. The suggested changes would require the Secretary to obtain a search warrant in exigent cases where documents might be hidden or destroyed

Full Text of Rep. Arney's Letter:
<http://www.hipaadvisory.com/news/2001/armey0503.htm>

*** Gartner Survey: Industry Moving Too Slowly on HIPAA ***

With less than 18 months remaining until the compliance deadline for the HIPAA transaction regulations, most healthcare organizations (HCOs) have not completed assessments of their current environments and risks, according to a recent survey by Gartner, Inc. According to Gartner, if the HIPAA effective date is not delayed, HCOs must aggressively begin compliance efforts within the next three months or miss the deadline and risk incurring high penalties and financial damage.

The survey showed that HCOs have at least started the early awareness tasks required for HIPAA compliance. Moreover, according to Gartner, a finding that almost one-half of HIPAA compliance officers now report to either their CEO or a senior management committee offers evidence of an increasing understanding of HIPAA's strategic significance to many HCOs (as opposed to it being viewed solely as a conformance issue, such as the year 2000 crisis).

For more information, go to:

<http://www.hipaadvisory.com/news/2001/gartner0502.htm>

*** First HIPAA Privacy Guideline Due in May ***

DHHS Secretary Tommy Thompson announced on April 26th that the first guideline to clarify the HIPAA Privacy Rule will be issued in May. Speaking before the House Committee on Energy and Commerce's Subcommittee on Health, Thompson stated that DHHS plans to "develop guidelines to clarify certain points of confusion about the rule," and is also considering "where modifications to the rule may be needed to ensure that quality of care does not suffer inadvertently." He noted that the concerns of 11,000+ commenters to the Privacy Rule, including interest groups and health care leaders, are being considered in formulating DHHS guidance and modifications.

According to an article in Health Data Management, the guideline will clarify several provisions in the rule, such as the right of family members or friends to pick up a person's prescription. The guideline likely also will address concerns regarding oral communications, patient consent provisions and the "minimum necessary" disclosure of information, among other issues.

For more information, go to:

<http://www.hipaadvisory.com/news/2001/PrivGuideline4-26.htm>

*** Congressmen Prepare to Pressure DHHS on Privacy ***

Members of Congress are circulating a letter, urging HHS Secretary Tommy Thompson to fix the HIPAA privacy rule and support additional funds to help hospitals comply. Reps. Greg Walden (R-OR), Cal Dooley (D-CA), Mike Pence (R-IN), and David Phelps (D-IL), are circulating "Dear Colleague" letters on Capitol Hill this week, asking their colleagues to sign on to letter asking the Bush administration to change the privacy rules now.

The letter asks for changes to the HIPAA Privacy rule that became effective on April 14th. Federal funding for compliance is also requested.

According to the American Hospital Association (AHA), 26 House members have signed the letter.

For both the "Dear Colleague" letter and the letter to Sec. Thompson: <http://www.hipaadvisory.com/news/2001/house0503.htm>

*** Bush Wants Medical Mistakes Listed on Net ***

The Bush administration is working to create an Internet-based clearinghouse of medical mistakes made by doctors and hospitals, with the intention of helping them avoid such errors in the future. Health care providers could use the Internet to report information to the federal government or to state and private-sector regulators.

=====

4 / H I P A A d v i s o r : Legal Q/A with Steve Fox, J.D.

*** Of Affiliates and Associates ***

QUESTION: We are a hospital that is affiliated with a number of other health facilities in our community including mammography, occupational health, and nursing care facilities. We do not own any of the health facilities and each of the affiliated entities has a separate Board of Directors but there is representation from all of the affiliates on each of the boards. The affiliation allows each facility to offer its patients a seamless network of fully integrated care. Accordingly, some of our information systems are shared. These shared systems contain several computer applications, some containing protected health information, that do not have segregated databases. Do we need to enter into some sort of contract with each affiliate in order to be in compliance with the privacy regulation under HIPAA?

ANSWER: No. The affiliation you have described is not a business associate relationship as defined in the privacy regulation (the

"Rule") and therefore, the parties are not obligated to execute a business associate agreement.

In order to ensure continuity in the care and protection of individually identifiable health information, the Rule requires covered entities to impose certain contractual obligations on business associates that perform functions or activities on behalf of covered entities. Although the Rule clearly states that covered entities may perform the function of a business associate, the mere fact that two covered entities share certain information systems does not make either of the covered entities a business associate of the other.

Affiliations like the one you have described are called "organized health care arrangements" under the Rule. Organized health care arrangements are clinically or operationally integrated care settings in which individuals receive health care from more than one of the participating health care providers.

Health care providers are generally required to obtain an individual's consent before using or disclosing that individual's protected health information. However, individuals can consent to the use of their protected health information by the entire membership of any one organized health care arrangement instead of individually consenting to each provider's use of such data. Entities that participate in organized health care arrangements may develop joint consent forms for this purpose. Your hospital may want to work with all of the affiliates to develop a joint consent form.

Finally, it is important to note that shared systems contain electronically maintained health information and are therefore subject to HIPAA's security regulation. Although the final security regulation has not been released, the proposed regulation requires, among other safeguards, information access controls and entity authentication. Accordingly, any shared systems should either have segregated databases or their use should be governed by a chain of trust agreement in order to insure that the same level of security is maintained by all of the affiliates.

To read past HIPAAAdvisor articles, go to:

<http://www.hipaadvisory.com/action/HIPAAAdvisor.htm>

Steve Fox, J.D., is a partner at the Washington, D.C. office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, an associate at Pepper Hamilton. Pepper Hamilton LLP is a multi-practice law firm with more than 400 lawyers in ten offices.
<http://www.pepperlaw.com/>

Disclaimer: This information is general in nature and should not be relied upon as legal advice. Only your attorney is qualified to evaluate your specific situation and provide you with customized

advice.

=====

5 / H I P A A v i e w : Vendors and HIPAA Compliance -- Reality Knocks
by Roy Rada, MD, PhD, Author of HIPAA@IT

*** How HIPAA-Compliant can Any Technology Be? ***

American history has witnessed a myriad of compliance activities; some we might point with pride to, such as the 1906 Pure Food and Drug Act, resulting from Dr. Harvey Wiley's efforts to regulate the content of food. However, the role of government in regulating business in the US has often been accompanied by controversy and debate.

HIPAA has proved to be another battleground for compliance. Without going further into the history, politics, law, or ethics of compliance, let's address the seemingly simple question of whether information technology can be compliant with HIPAA.

How many times have you heard a vendor tout 'my technology is HIPAA compliant'? Some providers and payers are demanding to get HIPAA compliant technology. Claims are commonly made by salespeople that their product is HIPAA compliant. What's the scoop here?

Direct compliance with HIPAA's administrative simplification provisions is not practical because the law itself is too indirect. It calls for rules to be developed and enforced by the executive branch of the federal government. Furthermore, the rules are diverse and cover, at least, transactions, privacy, and in proposed-form security.

TRANSACTIONS RULE

Might an IT vendor rightfully claim to be compliant with the Transactions Rule? 'Transaction' refers in the HIPAA-context to provider-payer transaction. The Transactions Rule calls for compliance with certain standards, particularly X12 formats. A health care provider might want to use information systems that support message formats to payers that are compliant with X12, and a vendor could claim to provide such X12-compliant forms.

This isn't to say that the entity buying the technology would have an instant fix to its 'Transactions' compliance problem. The Transactions Rule goes beyond the X12 formats to specify the codes that have to be used inside the fields of the format. Achieving compliance with some coding requirements may entail changes in behavior. However, technology could enforce the use of Transaction Rule formats and codes and thus support compliance with the HIPAA transaction rule.

PRIVACY RULE

Privacy calls for changes in the way an entity manipulates information. This is largely an administrative rather than a technical issue. However, a technology can support the options for manipulating information and be a vital support of the entity behavior. The technology should support behavior consistent with the Privacy Rule.

The Privacy Rule calls for information systems that represent and audit workflow. Exactly what the workflow should be is not precisely defined. The approach of the Privacy Rule is like the ISO (the pre-eminent international standards organization) approach to quality in ISO 9000. ISO 9000 says that an organization should be clear in its goals and work consistently to those goals. ISO 9000 does not say what the organization-specific goals should be, but an organization can be certified as ISO 9000 compliant. To be ISO 9000 compliant an organization must document its objectives and document that its activities take it towards its objectives -- nothing more. The Privacy Rule goes beyond ISO 9000 in specifying broadly what some of the privacy objectives are but then asks entities to be quality organizations as respect to those objectives.

Entities must document working towards privacy objectives. Certifying compliance for privacy would require an analysis of the organizational manual and the way the organization implemented its manual. An IT tool should help a health care entity have and follow the appropriate organizational manual but the tool would not make the entity HIPAA compliant.

SECURITY RULE

No security rule has been finalized for HIPAA. Yet, security is the topic that comes closest to what an IT vendor feels is the special turf of the vendor. The typical healthcare entity may be violating various security mandates, such as transmitting information over the Internet in encrypted form. A vendor can provide tools that encrypt messages before sending them across the Internet.

The proposed security rule gives objectives of secure transmissions, reliable authentication, contingency preparations, and much more. However, the proposed rule gives flexibility to organizations in their choice of ways to achieve the objectives and is neutral about particular technologies. The compliance argument about security is not dissimilar to the argument about privacy: when an organization uses a technology in a certain way to reach a certain objective, then the organization will have behaved in a compliant way as regards that HIPAA security objective.

OVERALL...

The bottom line is that Administrative Simplification is about Administration, and technology can support that administration -- but not replace it. An information technology vendor should help its clients understand what parts of HIPAA compliance are supported by the

vendor's technology. But it should not claim that the technology is HIPAA compliant.

Read more articles by Roy Rada and order his book,
HIPAA@IT:Health Information Transactions, Privacy & Security
published by HIMSS, 2001
<http://www.hipaadvisory.com/action/atit/>

=====

Informative HIPAA Audioconferences and tapes available at:
<http://www.hipaadvisory.com/action/learn.htm>

There's still time to sign up for the Privacy and Unique IDs
HIPAA-in-the-Trenches audioconference!
<http://www.hipaadvisory.com/action/signup/trenches/>

=====

BRING YOUR HIPAA QUESTIONS AND IDEAS TO LIFE AT...H I P A A l i v e!

Join 3100 other thinkers, planners, learners and lurkers
who are already members of our sister e-mail discussion list.
We almost make HIPAA fun! Almost.
Subscribe now at: <http://www.hipaadvisory.com/live/>

=====

RAISE YOUR ORGANIZATION'S HIPAAWARENESS WITH H I P A A n o t e s !

Over 4500 industry members are already receiving a weekly byte of
HIPAA. Your HIPAAnote is suitable for publishing on your
organization's intranet or newsletter & comes free to your e-mailbox.
Subscribe now at: <http://www.hipaadvisory.com/notes/>

=====

COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit <http://www.hipaadvisory.com/alert/>
ARCHIVES: <http://www.hipaadvisory.com/alert/newsarchives.htm>

=====

Copyright 2001, Phoenix Health Systems, Inc. All Rights Reserved.
Reprint by permission only.
<http://www.phoenixhealth.com> 301-869-7300

=====

FORWARD this posting to interested associates, who may subscribe free to HIPAAAlert
at:
<http://www.hipaadvisory.com/alert/>
Subscribe to our free discussion list at:
<http://www.hipaadvisory.com/live/>

Get a weekly byte of HIPAA at:
<http://www.hipaadvisory.com/notes/>

You are currently subscribed to hipaalert as:kmckinst@dmhhq.state.ca.us
To unsubscribe send a blank email to leave-hipaalert-85079900@lists.hipaalert.com